Deutscher Bundestag **Drucksache 16/7891**

16. Wahlperiode 23. 01. 2008

Unterrichtung

durch die Bundesregierung

Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums des Innern vom 23. Januar 2008 gemäß Beschluss vom 29. März 2007 (Bundestagsdrucksache 16/4882).

Seite

I. Einleitung

A. Bezug

„RFID“ ist die Abkürzung für „Radiofrequenz-Identifikation“. Unter „RFID-Technologie“ versteht man Verfahren zur kontaktlosen Identifizierung von Objekten oder Personen per Funk. RFID-Systeme bestehen aus zwei Komponenten: Einem elektronischen Mikrochip (sog. „Tag“) mit Antenne, auf dem Daten gespeichert werden können, und einem Lesegerät, das die gespeicherten Daten erfasst und in eine Datenbank überträgt.

Der vorliegende Bericht des Bundesministeriums des Innern bezieht sich auf die Entschließung des 16. Deutschen Bundestages vom 29. März 2007 (Plenarprotokoll 16/91, S. 9248 i. V. m. Bundestagsdrucksache 16/4882) zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Bundestagsdrucksache 15/5252), in der die Bundesregierung aufgefordert worden ist, den Bundestag über die Aktivitäten und Planungen sowie einen möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie zu unterrichten. In Nummer 7 der Entschließung (Bundestagsdrucksache 16/4882, S. 3) heißt es:

„Der Deutsche Bundestag hat bereits in seiner Entschließung zum 19. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Bundestagsdrucksache 15/4597) die Bedeutung von Entwicklung und Einsatz datenschutzfreundlicher Technologien hervorgehoben (Nr. 5). Er fordert die Bundesregierung auf, sich für die Gewährleistung des Daten- und Verbraucherschutzes bei der Nutzung der RFID-Technologie einzusetzen. Insbesondere muss dafür Sorge getragen werden, dass die Betroffenen umfassend über den Einsatz, Verwendungszweck und den Inhalt von RFID-Tags informiert werden. Es muss die Möglichkeit bestehen, die im Handel verwendeten RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, wenn Daten nicht mehr erforderlich sind. Ferner muss gewährleistet werden, dass Daten von RFID-Tags aus verschiedenen Produkten nur so verarbeitet werden, dass keine heimlichen personenbezogenen Verhaltens-, Nutzungs- und Bewegungsprofile erstellt werden können. Die Bundesregierung wird aufgefordert, dem Deutschen Bundestag noch in diesem Jahr über ihre Aktivitäten und Planungen und einen möglichen gesetzgeberischen Handlungsbedarf zu berichten (20. TB, Nr. 4.2.1).“

B. Gang der Darstellung

In Teil 1 des Berichts werden die wesentlichen Grundzüge von RFID dargestellt.

- Technische Grundlagen: Wie funktioniert RFID?
- Anwendungsgebiete: Wo wird heute bereits RFID-Technologie eingesetzt?
- Zukunftsperspektiven: Wird RFID sich zum Massenphänomen entwickeln?
- Chancen und Risiken: Welche Vor- und Nachteile bringt RFID im Vergleich zu anderen Identifikationssystemen?

Teil 2 erörtert den Einsatz von RFID nach der aktuellen Rechtslage. Zugleich werden die wesentlichen Risiken für den Schutz personenbezogener Daten aufgezeigt und mögliche Lösungswege angesprochen.

- Erhebung, Verarbeitung und Nutzung personenbezogener Daten: In welcher Form werden durch den Einsatz von RFID personenbezogene Daten verarbeitet? Bietet das geltende Recht hinreichenden Schutz für die Betroffenen?
- Löschung personenbezogener Daten: Wann, wo und in welcher Form müssen Löschungsmöglichkeiten für die auf den Tags gespeicherten Daten zur Verfügung gestellt werden, damit der Verbraucher die Kontrolle über seine personenbezogenen Daten behält?

Teil 3 des Berichts schildert die derzeitigen nationalen und europäischen Aktivitäten zum Datenschutz bei RFID.

- Aktueller Stand: Welche Aktivitäten gibt es derzeit auf nationaler und europäischer Ebene? Wie verhält sich die Wirtschaft zur datenschutzrechtlichen Problematik von RFID?

In Teil 4 werden die wesentlichen Handlungsoptionen zur Lösung der datenschutzrechtlichen Problematik von RFID erörtert.

- Weitere Vorgehensweise: Welche gesetzgeberischen Maßnahmen wären denkbar und wo lägen ihre Vor- und Nachteile? Wäre eine Selbstverpflichtung der Wirtschaft eine realistische Alternative?

Der fünfte und letzte Teil enthält Empfehlungen zur weiteren Vorgehensweise.

Insgesamt konzentriert sich der vorliegende Bericht – der Anforderung des Deutschen Bundestages entsprechend – auf die datenschutzrechtlichen Aspekte von RFID. Gleichwohl ist der Bundesregierung bewusst, dass ein vermehrter Einsatz von RFID-Technologie auch Auswirkungen auf die Bereiche Wirtschaft, Umwelt, Gesundheit, Forschung und Verbraucherschutz haben kann. Diese Auswirkungen bedürften indessen aufgrund ihrer Komplexität einer eigenen, differenzierten Betrachtung.

II. Teil 1: Wesentliche Grundzüge von RFID

„RFID“ ist die Abkürzung für „Radiofrequenz-Identifikation“ (Radio Frequency Identification). Unter „RFID-Technologie“ versteht man Verfahren zur kontaktlosen Identifizierung von Objekten per Funk. RFID zählt damit zu den sog. Automatic Identification (Auto-ID)-Systemen.

A. Funktionsweise und Stand der Technik

RFID-Systeme bestehen aus zwei Komponenten: Einem Transponder (dem sog. „Tag“) und einem Lesegerät (dem sog. „Reader“). Der Transponder wird auf dem zu kennzeichnenden Trägerobjekt angebracht. Er enthält einen

elektronischen Mikrochip zur Datenspeicherung sowie eine Antenne, mit der Funkwellen gesendet und empfangen werden können. Das Lesegerät besteht ebenfalls aus Sender, Empfänger und Antenne. Gelangt ein „getagtes“ Objekt in die Sendereichweite eines Readers, können die auf dem Tag gespeicherten Daten ausgelesen und zur weiteren Verarbeitung in eine Hintergrunddatenbank (sog. „Back-end“) übertragen werden. Je nach System unterscheidet man zwischen „read-only“ und „read and write“-Tags. Die Größe der Tags ist unterschiedlich, kann heute jedoch bereits weit unter einem Quadratmillimeter liegen.

Sendereichweite und Speicherkapazität von RFID-Systemen sind abhängig von der gewählten Funkfrequenz und der Ausstattung der Tags. Man unterscheidet insoweit passive und aktive Tags.

Passive Tags besitzen keine eigene Energiequelle. Sie werden durch induktive Kopplung vom Reader aus mit Energie versorgt. Der Reader erzeugt hierzu ein starkes elektromagnetisches Feld, das von der Empfängerantenne des Transponders aufgenommen und zur Übertragung der gespeicherten Daten an den Reader genutzt wird. Aktive Tags besitzen im Gegensatz dazu eine eigene Energiequelle in Form einer Batterie. Verglichen mit passiven Tags verfügen sie über eine höhere Speicherkapazität und Sendereichweite, sind allerdings auch deutlich teurer, größer und von geringerer Lebensdauer.

Lesegeräte erfassen automatisch alle in ihre Empfangsreichweite gelangenden Tags, unabhängig davon, ob diese gezielt oder zufällig in ihre Nähe gebracht werden. Solange ein Chip nicht deaktiviert ist, kann er mithin bis zum Ende seiner Lebensdauer von jedem Reader ausgelesen werden. Ob die übertragenen Daten für den Verwender des jeweiligen Readers tatsächlich verwertbar sind, hängt allerdings von ihrem Inhalt und Verschlüsselungsgrad ab.

Hinsichtlich der Funkfrequenzen haben sich für den RFID-Einsatz die Frequenzbereiche von unter 135 kHz (Niedrigfrequenzbereich), 13,56 MHz (Hochfrequenzbereich), 866 bis 960 MHz (Ultrahochfrequenzbereich – UHF) und 2,45 GHz (Mikrowellenbereich) durchgesetzt. Niedrigfrequenzsysteme besitzen nur geringe Reichweiten, bieten bei einigen Materialien (z. B. Wasser) aber bessere Durchdringungswerte und sind vergleichsweise preiswert herzustellen. Systeme auf höheren Frequenzen verfügen über längere Reichweiten, sind unempfindlicher gegenüber elektromagnetischen Störfeldern und erlauben den Transfer größerer Datenmengen. Die Auswahl des Frequenzbereichs hängt daher maßgeblich vom jeweiligen Einsatzgebiet des Systems ab.

Passive Tags besitzen im Niedrigfrequenzbereich lediglich eine Reichweite von wenigen Zentimetern. Im Hochfrequenzbereich werden bis zu 3 m erreicht. Etwa 90 Prozent aller derzeit eingesetzten RFID-Systeme arbeiten mit Reichweiten von maximal einem Meter.

Die Sendereichweite von aktiven Tags beträgt im Regelfall bis zu 30 m. In Ausnahmefällen und bei Verwendung eines extrem hohen Frequenzbereichs können Reichweiten bis zu 1 000 m erreicht werden.

Darüber hinaus können aktive RFID-Chips mit Sensoren verknüpft werden (sog. „Sensor-Tags“) und dadurch Messwerte, z. B. zu Temperatur, Feuchtigkeit oder Erschütterungen, erheben und speichern.

B. Aktuelle Einsatzgebiete von RFID

Die Einsatzmöglichkeiten für RFID-Systeme sind vielfältig. Sie eignen sich grundsätzlich für alle Bereiche, in denen die automatische Kennzeichnung, Erkennung, Registrierung, Lagerung und Überwachung oder der automatische Transport von Objekten erforderlich sind.

Auf folgenden Gebieten findet RFID-Technologie derzeit bereits in einigem Umfang Anwendung:

Logistik/Lagermanagement/Transport und Electronic Product Code

Insbesondere im Handel, aber auch bei Postdienstleistungen und in der Gepäckabfertigung an Flughäfen, wird RFID zur Steuerung, Überwachung und Optimierung von Liefer- und Lagerungsprozessen eingesetzt. Hierzu werden Güter, z. B. Waren oder Wareneinheiten mit einem RFID-Chip „getagt“, der einen individuellen Produktcode enthält. Über Lesegeräte an den unterschiedlichen Stationen der Lieferkette oder des Transportweges kann z. B. der Weg eines Trägerobjekts vom Hersteller bis zum Endkunden automatisch überwacht und gesteuert werden.

Je nach Frequenzbereich erkennen RFID-Lesegeräte etwa 200 Tags pro Sekunde. Lagerbestände und Warenfluss lassen sich daher in kürzester Zeit automatisch erfassen und optimieren. Bei sensiblen Gütern, beispielsweise solchen die eine geschlossene Kühlkette benötigen, können über Sensor-Chips zudem die Umweltbedingungen überwacht, protokolliert und nachgewiesen werden. Genutzt wird diese Technik teilweise bereits für den Transport von Blutkonserven, Pflanzen und Gemüse.

Um RFID-Systeme auch für den internationalen Warenverkehr nutzbar zu machen, hat die Non-profit-Organisation EPCglobal einen weltweit standardisierten Produktcode entwickelt, den sog. „EPC“ (Electronic Product Code). Der EPC soll erstmals jeder Ware bis hinunter zur einzelnen Verpackungseinheit eine global einmalige Identifikationsnummer zuweisen und zukünftig als neuer Nummernstandard das EAN (European Article Number)-System der derzeit noch handelsüblichen Strichcode-Etiketten ersetzen. RFID-Tags haben gegenüber Strichcode-Etiketten zudem den Vorteil, dass sie keinen Sichtkontakt zum Lesegerät benötigen, daher in ein Objekt integriert werden können, und unempfindlicher gegenüber Umwelteinflüssen wie Schmutz, Staub oder Licht sind.

Ebenso wie bei EAN zahlen die Teilnehmer des EPC-Systems eine umsatzabhängige Aufnahme- und Jahresgebühr. Darüber hinaus steht EPC für ein internationales Informationsnetzwerk, das den teilnehmenden Unternehmen einen schnellen und sicheren Austausch von Produktdaten ermöglichen soll. Hierzu betreibt EPCglo-

bal u. a. einen „Object Naming Service“ (ONS), eine Art Adressbuch, über das anhand des jeweiligen Produktcodes abgefragt werden kann, wo der Nummerngeber weitere Produktinformationen bereithält. Das Netzwerk basiert auf Forschungs- und Entwicklungsarbeiten, die vom Auto-ID Center des Massachusetts Institute of Technology (MIT) initiiert wurden, und zählt derzeit weltweit etwa 850 Unternehmen. Auf deutscher Seite wird EPCglobal durch das Industriestandardisierungsgremium GS1 Germany vertreten.

Prozesskontrolle/Produktion

In der Produktion wird RFID zur Kontrolle automatisierter Arbeitsprozesse eingesetzt. Beispielsweise steuert die Automobilindustrie ihre Fertigungslinien über RFID-Chips, die an den Werkstücken angebracht sind und den einzelnen Stationen signalisieren, welche Farbe oder Ausstattung ein Fahrzeug erhalten soll.

Zahlungssysteme/Zugangskontrolle

Ein weiterer großer Anwendungsbereich von RFID-Technologie sind Zahlungs- und Zugangskontrollsysteme (z. B. Skipässe, Mitgliedsausweise, Eintritts-, Kunden-, Schlüssel- und Signaturkarten, Geräte zur Fernablesung des Wärmeverbrauchs nach der Heizkostenverordnung). Unter anderem waren die Tickets zur Fußball-WM 2006 mit RFID-Chips gekennzeichnet. Diskotheken, die ihren Stammkunden auf Wunsch RFID-Chips unter die Haut applizieren, sind bisher jedoch auf das Ausland beschränkte, absolute Einzelfälle geblieben.

Wegfahrsperren

Weite Verbreitung hat RFID als Wegfahrsperre bei Kraftfahrzeugen gefunden. Der Tag befindet sich bei dieser Applikation im Autoschlüssel, das Lesegerät im Zündschloss.

Landwirtschaft/Qualitätskontrolle

Ähnlich wie im Warenhandel werden auch Tiere bereits vielfach mit RFID-Chips und weltweit einmaliger Identifikationsnummer gekennzeichnet. Große Tierbestände können dadurch schnell erfasst, entlaufene Haustiere oder Brieftauben eindeutig identifiziert werden. Außerdem ermöglicht die Kennzeichnung eine lückenlose Herkunftskontrolle (z. B. von Fleischwaren) und dient damit dem Verbraucherschutz, der Seuchenbekämpfung und der Qualitätskontrolle.

Arbeitswelt

In einigen Betrieben und Stellen der öffentlichen Verwaltung wird RFID (zumeist in Form von Chipkarten) zur Zeiterfassung, Zugangskontrolle und Authentifizierung eingesetzt. Teilweise werden auch Routinerundgänge z. B. des Sicherheits- oder Wartungspersonals mithilfe von Lesegeräten überwacht. Die Anwendung von RFID-Technologie zur Aufenthaltsbestimmung von Arbeitnehmern in Gefahrenbereichen wird ebenfalls diskutiert, befindet sich jedoch noch weitgehend in der Testphase. Insgesamt unterscheidet sich die mit dem Einsatz von RFID in der Arbeitswelt einhergehende Überwachungsproblematik rechtlich im Kern nicht von den in diesem Zusammenhang bereits bekannten und diskutierten Problemstellungen.

Auf folgenden Gebieten werden RFID-Systeme derzeit in Form von Modellversuchen, Pilotprojekten und Testläufen erprobt:

Endkundenbereich

Im Endkundenbereich laufen bei verschiedenen Einzelhandelsketten Modellversuche zu RFID-gestützten Kassensystemen und sog. „intelligenten Regalen“. RFID-Kassen erfassen alle getagten Produkte in einem Einkaufskorb gleichzeitig und helfen daher, die Bezahlvorgänge deutlich zu beschleunigen. „Intelligente Regale“ melden selbstständig, wann bestimmte Waren nachgeliefert werden müssen. Insgesamt befindet sich die Kennzeichnung von Konsumgütern jedoch noch in der Anfangsphase und erfolgt meist nur zu logistischen Zwecken. Getagt werden hauptsächlich Paletten und Umkartons, die im Regelfall nicht in die Verbrauchersphäre gelangen. Die Kennzeichnung von Einzelartikeln (das sog. „item-tagging“) wird bisher nur testweise in wenigen Verkaufsstellen großer Einzelhandelsketten praktiziert. In geringem Umfang werden RFID-Chips zudem zur Diebstahlssicherung und Qualitätskontrolle eingesetzt. Zukünftig sollen darüber hinaus Produktinformationsterminals getestet werden, über die der Kunde z. B. Angaben zu Inhaltsstoffen, Herkunft oder Kombinationsmöglichkeiten bestimmter Artikel abrufen kann. Ansonsten geht die Nutzung von RFID im Endkundenbereich derzeit noch nicht über die Funktionalitäten des Barcodes hinaus.

ÖPNV

In einigen Kommunen werden RFID-Systeme für den ÖPNV-Bereich erprobt. Der Fahrgast hält beim Ein- und Aussteigen ein wiederaufladbares RFID-Ticket mit Zahlungsfunktion vor ein Lesegerät, das automatisch den Fahrpreis berechnet und vom Kartenguthaben abbucht.

Archivierungssysteme

Gleiches gilt für die RFID-Kennzeichnung von Bibliotheks- und Archivbeständen. Auch hier wird in einigen Pilotprojekten getestet, inwieweit sich Bestandserfassung, Diebstahlschutz und Ausleihvorgänge durch den Einsatz von RFID optimieren lassen.

Identitäts- und Echtheitsnachweis/Bekämpfung von Diebstahl und Produktpiraterie

In diese Kategorie fallen u. a. RFID-Anwendungen auf dem ePass, auf Veranstaltungstickets sowie auf Arzneimitteln und Luxusartikeln.

Sport

Im Sport wird RFID vor allem bei Marathonwettbewerben eingesetzt. Mithilfe von RFID-Transpondern an den Laufschuhen der Teilnehmer lässt sich nachverfolgen, ob und wann ein Läufer einen bestimmten Streckenabschnitt passiert hat.

Gesundheitssystem

Im Gesundheitsbereich beschränkt sich der Einsatz von RFID ebenfalls auf einige wenige Pilotprojekte. Beispielsweise erhalten im Klinikum Saarbrücken Patienten Chip-Armbänder, auf denen die Patientennummer gespeichert ist. Dadurch sollen die Auslastung der medizinischen Geräte optimiert, Verwechslungen verhindert und Wartezeiten verkürzt werden. Teilweise werden auch Verbands- und Operationsmaterialien zur leichteren Bestandsverwaltung mit Tags versehen.

Eine Reihe weiterer Anwendungsmöglichkeiten von RFID-Technologie werden derzeit diskutiert (darunter z. B. kommunale Mauterhebungssysteme „Citymaut“, Feuermeldesysteme, Sensor-Chips zur Überwachung des Blutzuckerspiegels, Wertstofferkennung in der Abfallwirtschaft), sind – zumindest in Deutschland – jedoch noch nicht zur praktischen Umsetzung gelangt.

C. Entwicklungsprognose

RFID ist eine Schlüssel- und Querschnittstechnologie, die in den kommenden Jahren wesentlich an Bedeutung gewinnen wird.

Eine im Auftrag des Bundesministeriums für Wirtschaft und Technologie erstellte Studie kommt zu dem Ergebnis, dass im Jahr 2010 ca. 8 Prozent der Bruttowertschöpfung in wichtigen Bereichen des produzierenden Gewerbes, des Handels, des Verkehrs sowie der privaten und öffentlichen Dienstleister von RFID beeinflusst sein werden.

Kurz- und mittelfristig wird RFID dabei vor allem im Logistik- und Lagermanagement sowie in der Fertigung weitere Verbreitung finden. So soll die Kennzeichnung von Transportbehältern bereits 2010 flächendeckend auf RFID-Tags umgestellt sein. Im gleichen Zeitraum wird sich die Zahl der RFID-Anwender in der Automobilindustrie voraussichtlich verdoppeln.

In anderen Wirtschaftsbereichen und insbesondere im Mittelstand wird RFID dagegen erst mittel- bis langfristig eine größere Rolle spielen. Der „RFID-Hype“ der vergangenen Jahre hat sich hier merklich abgekühlt. Dies liegt zum einen an den noch zu hohen Produktionskosten der Tags. Zum anderen fehlt für viele Systemkomponenten noch die notwendige – auch internationale – Standardisierung. Vor allem die Einführung eines weltweit harmonisierten Frequenzspektrums stößt auf Schwierigkeiten, da Europa gerade im besonders nachgefragten UHF-Bereich nur begrenzte Bandbreiten zur Verfügung stellen kann.

Auf welchen Gebieten und vor allem in welchem zeitlichen Rahmen RFID-Applikationen über den Produktions- und Logistikbereich hinaus signifikante Verbreitung finden werden, ist derzeit noch nicht konkret absehbar. Eine flächendeckende Einführung von miteinander kompatiblen Lesegeräten wird – wenn überhaupt – allenfalls auf lange Sicht entstehen.

Nach derzeitigem Kenntnisstand ist zu vermuten, dass Endverbraucher vor dem Jahr 2015 nicht flächendeckend mit RFID konfrontiert sein werden. Die Kennzeichnung von Konsumgütern mit RFID-Tags befindet sich gegenwärtig erst in der Anfangsphase und wird den EAN-Strichcode nur langsam ablösen. Der Einsatz von „intelligenten Regalen“, Informationsterminals und RFID-gestützten Kassensystemen reicht über das Versuchsstadium noch nicht hinaus. Mittelfristig werden allenfalls die größeren Einzelhandelsketten vermehrt solche Applikationen einführen. Gleiches gilt für den Einsatz von RFID-Tickets im ÖPNV-Bereich. Eine flächendeckende Umstellung auf RFID ist dort schon aus Kostengründen in näherer Zukunft nicht zu erwarten.

Verbraucher werden daher auch mittelfristig im Wesentlichen mit den bereits etablierten Anwendungsformen von RFID (Wegfahrsperre, Veranstaltungs-Ticketing, Zugangskontrollen, ePass) konfrontiert sein.

D. Chancen und Risiken

Große Chancen bietet RFID vor allem für die deutsche Wirtschaft.

Deutschland ist derzeit – neben Frankreich und Großbritannien – Vorreiter bei der Entwicklung, Erprobung und Umsetzung von RFID-Anwendungen. Für die deutschen Hersteller von RFID-Komponenten wird bis 2010 eine Umsatzsteigerung auf etwa 1,4 Mrd. Euro Gesamtumsatz (2006: ca. 914 Mio. Euro) prognostiziert.

Darüber hinaus bietet RFID erhebliches Potential zur Effizienz- und Qualitätssteigerung vor allem in den Bereichen Logistik und Prozesskontrolle. So werden in der Automobilindustrie durch den vermehrten Einsatz von RFID bis 2010 Produktivitätseffekte von 2,42 Mrd. Euro (2006: 0,75 Mrd. Euro) erwartet. Die flächendeckende Kennzeichnung von Transportbehältern mit RFID-Tags soll zu Effizienzsteigerungen von 5 bis 10 Prozent führen.

Verantwortungsvoll eingesetzt versprechen RFID-Systeme auch große Vorteile für Verbraucher. Zu nennen sind hier vor allem beschleunigte Bezahlvorgänge, bessere Rückverfolgbarkeit von Produkten sowie höhere Produktsicherheit und -qualität. In einigen Bereichen ist der Einsatz von RFID-Technologie auf Verbraucherseite bereits allgemein akzeptiert (z. B. bei Mitglieds- und Eintrittskarten, Skipässen, Wegfahrsperren oder Zugangskontrollen).

Dennoch birgt der Einsatz von RFID auch gewisse Risiken für das informationelle Selbstbestimmungsrecht des Einzelnen und wird daher insbesondere auf Daten- und Verbraucherschutzseite kontrovers diskutiert. Verbraucherschutzverbände wie auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit warnen regelmäßig davor, dass die RFID-gestützte Verarbeitung personenbezogener Daten für Betroffene kaum kontrol-

lierbar ist. Insbesondere bestehe die Gefahr, dass Dienstleister über heimlich ausgelesene RFID-Tags detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile erstellen, um ihre Marketingstrategien zu optimieren. In manchen Kreisen werden sogar „Big-Brother-Szenarien“ einer allgegenwärtigen Überwachung befürchtet (s. hierzu auch Ziff. III C).

Letztere sind angesichts der Tatsache, dass mit einem flächendeckenden Netz von Lesegeräten allenfalls sehr langfristig zu rechnen ist, noch völlig unrealistisch. Kurz- und mittelfristig wird die RFID-basierte Verarbeitung personenbezogener Daten kaum über das hinausgehen, was heute bereits über Kunden- und Kreditkarten, Barcode und Überwachungskameras möglich – und üblich – ist. Zudem sind viele in der Verbrauchersphäre anzutreffenden RFID-Systeme auf den unmittelbaren Nahbereich ausgelegt. Sie erkennen mithin nur solche Tags, die Betroffene direkt vor das Lesegerät halten, nicht dagegen Chips, die sich an weiter entfernter Stelle in der Kleidung oder im Geldbeutel befinden.

Abgesehen davon sind die Befürchtungen auf Daten- und Verbraucherschutzseite jedoch nicht unbegründet. Die besondere Funktionsweise von RFID führt dazu, dass Datenverarbeitungsvorgänge für Betroffene nicht ohne weiteres erkennbar werden und daher ohne entsprechende Schutzmaßnahmen kaum kontrollierbar sind. Dies ergibt sich daraus, dass

- RFID-Tags aufgrund ihrer geringen Größe für Verbraucher quasi unsichtbar sind,
- Lesegeräte automatisch alle in ihre Reichweite gelangenden Tags erfassen – auch solche fremder oder früherer Verwender –, soweit sie technisch kompatibel sind,
- der Leseprozess sichtkontaktlos erfolgt und
- bei jedem Leseprozess die Möglichkeit besteht, dass an sich neutrale Speicherdaten im Back-end-System mit personenbezogenen Angaben zusammengeführt und auf diese Weise selbst zu personenbezogenen Daten werden.

Ausgehend von diesen Spezifika ist mithin zu fragen, welche rechtlichen und technischen Datenschutzinstrumentarien für den Einsatz von RFID aktuell zur Verfügung stehen, ob diese geeignet sind, das informationelle Selbstbestimmungsrecht der Betroffenen hinreichend abzusichern, und welche ergänzenden Schutzmaßnahmen gegebenenfalls empfehlenswert wären.

III. Teil 2: Die datenschutzrechtliche Bewertung von RFID-Applikationen

A. Gegenwärtige Rechtslage

Da für die RFID-basierte Erhebung, Verarbeitung und Nutzung von Daten keine bereichsspezifischen Normen existieren, bestimmt sich die Rechtslage nach den allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG).

Das BDSG konkretisiert auf einfachgesetzlicher Ebene das im „Volkszählungsurteil“ des Bundesverfassungsgerichts entwickelte „Recht auf informationelle Selbstbestimmung“ (BVerfGE 65,1 [41]). Dieses ist Bestandteil des durch Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts und damit wesentliche Ausprägung der Menschenwürde und der allgemeinen Handlungsfreiheit. Es verleiht dem Einzelnen die Befugnis, grundsätzlich selbst zu entscheiden, wann und in welchem Umfang er persönliche Lebenssachverhalte preisgeben möchte.

Das Recht auf informationelle Selbstbestimmung ist grundsätzlich ein Abwehrrecht des Bürgers gegen den Staat, es wirkt jedoch auch als objektive Schutznorm und verlangt gesetzgeberische und administrative Vorkehrungen mit dem Ziel, Beeinträchtigungen von Seiten nichtstaatlicher Dritter vorzubeugen. Nach der Rechtsprechung des Bundesverfassungsgerichts bedarf die informationelle Selbstbestimmung des Einzelnen in Zeiten moderner Datenverarbeitung – gerade angesichts der Möglichkeit zu umfassender Profilbildung – des besonderen Schutzes. Entsprechend unterwirft das BDSG den Umgang mit personenbezogenen Daten einer Reihe von Einwilligungs-, Transparenz- und Zweckbindungsregelungen.

Grundvoraussetzung für die Anwendbarkeit des BDSG ist das Erheben, Verarbeiten oder Nutzen personenbezogener Daten durch verantwortliche Stellen für nicht ausschließlich persönliche oder familiäre Tätigkeiten.

Dabei ist

- „Erheben“ das gezielte Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG,
- „Verarbeiten“ das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten, § 3 Abs. 4 Satz 1 BDSG,
- „Nutzen“ jede Verwendung personenbezogener Daten, die keine Verarbeitung ist (wie z. B. Kopieren oder Auswerten), § 3 Abs. 5 BDSG.

„Personenbezogene Daten“ sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“, § 3 Abs. 1 BDSG.

„Bestimmt“ ist eine Person, wenn – z. B. über eine unmittelbare Verknüpfung mit dem Namen und/oder sonstigen Identifizierungsmerkmalen der betroffenen Person – feststeht, dass sich die jeweiligen Daten nur auf diese Person und nicht auf eine andere beziehen.

„Bestimmbarkeit“ liegt vor, wenn die Daten erhebende Stelle mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln auf die hinter den Daten stehende Person schließen kann, die Daten mithin „personenbeziehbar“ sind.

Sind personenbezogene Daten betroffen, ist die Erhebung, Verarbeitung und Nutzung dieser Daten nur zulässig, wenn Betroffene entweder zuvor eingewilligt haben oder eine gesetzliche Vorschrift im BDSG oder Spezial-

gesetzen die Erhebung oder Verwendung der Daten erlaubt (§ 4 Abs. 1 BDSG). Zudem sind das Transparenzgebot sowie die Grundsätze der Zweckbindung und Erforderlichkeit zu beachten. Besondere Anforderungen gelten darüber hinaus für den Umgang mit sog. „sensitiven Daten“, d. h. Angaben zur rassischen und ethnischen Herkunft einer Person, zu politischen, religiösen und philosophischen Überzeugungen, zu Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.

Die Einwilligung bedarf grundsätzlich der Schriftform und muss auf der freien Entscheidung der Betroffenen beruhen. Diese sind daher auf den vorgesehenen Zweck der Datenerhebung, -verarbeitung und -nutzung sowie gegebenenfalls auf die Folgen der Verweigerung ihrer Einwilligung hinzuweisen. Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, ist sie besonders hervorzuheben (§ 4a BDSG).

Als gesetzlicher Erlaubnistatbestand für den Einsatz von RFID kommt insbesondere § 28 Abs. 1 BDSG in Betracht. Nach § 28 Abs. 1 Satz 1 Nr. 1 bis 3 BDSG ist die Erhebung und Verwendung personenbezogener Daten als Mittel zur Erfüllung eigener Geschäftszwecke zulässig,

– wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Verhältnisses mit den Betroffenen dient;

– soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung überwiegt;

– wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Dabei sind die Zwecke der Datenverarbeitung konkret festzulegen. Eine Nutzung zu anderen Zwecken als den festgelegten darf nur auf der Grundlage eines ausdrücklichen gesetzlichen Erlaubnistatbestands erfolgen. Eine entsprechende Erlaubnis besteht u. a. für die Nutzung zu Zwecken der Werbung, Markt- und Meinungsforschung, soweit die Betroffenen nicht widersprechen und zuvor über ihr Widerspruchsrecht aufgeklärt wurden, § 28 Abs. 3 Satz 1 Nr. 3, § 28 Abs. 4 BDSG.

Darüber hinaus muss der Umgang mit personenbezogenen Daten dem Transparenzgebot genügen, d. h. die verantwortliche Stelle hat die Pflicht, ihre Datenverarbeitungsvorgänge erkennbar zu machen, damit die Betroffenen selbst entscheiden können, wann und wem sie ihre Daten preisgeben.

Zur Absicherung des Transparenzgebots sieht das BDSG eine Reihe von Unterrichtungs-, Benachrichtigungs- und Auskunftspflichten der verantwortlichen Stellen vor. Erfolgt die Datenerhebung bei den Betroffenen selbst, sind sie über die Identität der die Daten erhebenden Stelle, die Zweckbestimmung der Datenerhebung, die Datenempfänger sowie über eventuelle gesetzliche Verpflichtungen zur Auskunftserteilung und die Folgen einer Auskunftsverweigerung zu unterrichten, § 4 Abs. 3 BDSG. Erfolgt die Datenspeicherung ohne Kenntnis der Betroffenen, sind sie entsprechend zu benachrichtigen, §§ 19a und 33 BDSG. Zudem gewähren §§ 19 und 34 BDSG den Betroffenen einen Anspruch auf grundsätzlich unentgeltliche Auskunft über die zu ihrer Person gespeicherten Daten, deren Zweckbestimmung und Empfänger.

Besondere Informationspflichten bestehen zudem beim Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien. Dies sind Datenträger, die an die Betroffenen ausgegeben werden und personenbezogene Daten nicht nur speichern, sondern auch automatisiert verarbeiten, wobei die Betroffenen den Verarbeitungsprozess lediglich durch Gebrauch oder Nichtgebrauch des Mediums beeinflussen können (z. B. Chipkarten, die automatisch Ort und Datum jeder Benutzung speichern). Wird ein solches Medium eingesetzt, muss die ausgebende Stelle die Betroffenen über ihre Identität und Anschrift sowie in allgemeinverständlicher Form über die Funktionsweise des Mediums aufklären. Zudem sind die Betroffenen darüber zu informieren, wie sie ihre Rechte auf Auskunft und Korrektur geltend machen können und welche Maßnahmen bei Verlust oder Zerstörung des Mediums zu treffen sind, § 6c BDSG.

Des Weiteren gelten die Grundsätze der Zweckbindung und Erforderlichkeit, d. h. personenbezogene Daten dürfen nur erhoben und verarbeitet werden, soweit sie für festgelegte, eindeutige und rechtmäßige Zwecke erforderlich sind. Technische Datenverarbeitungssysteme müssen so gestaltet sein, dass sie so wenige personenbezogene Daten wie möglich erheben. Unzulässig ist vor allem die sog. „Vorratsspeicherung“ zu unbestimmten Zwecken.

Personenbezogene Daten, die unter Missachtung der gesetzlichen Vorgaben gespeichert wurden, sind zu löschen, fehlerhafte Daten zu berichtigen, § 35 Abs. 1, Abs. 2 Satz 2 Nr. 1 BDSG.

Schließlich haben die verantwortlichen Stellen hinreichende Maßnahmen zur Datensicherung und Datenschutzkontrolle zu treffen, § 9 BDSG i. V. m. der Anlage zu § 9 BDSG. Insbesondere ist zu gewährleisten, dass ausschließlich berechtigte Personen auf das Datenverarbeitungssystem zugreifen und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Nach § 9 Satz 2 BDSG sind jedoch nur solche Maßnahmen erforderlich, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Verstöße gegen datenschutzrechtliche Vorschriften können mit einer Geldbuße von bis zu 250 000 Euro geahndet werden, § 43 BDSG. Bestimmte Handlungen sind zudem strafbewehrt, wenn sie gegen Entgelt, mit Bereicherungs- oder Schädigungsabsicht begangen werden, § 44 BDSG. Das Strafmaß ist Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Die Tat wird nur auf Antrag verfolgt.

B. Die Anwendbarkeit des bestehenden Datenschutzinstrumentariums auf RFID

Wie bereits beschrieben wird RFID in sehr unterschiedlichen Bereichen eingesetzt. Eine pauschale datenschutzrechtliche Bewertung dieser Technologie ist daher nicht möglich. Die Frage, ob und in welchem Umfang das bestehende Datenschutzregime auf RFID-Applikationen Anwendung findet – bzw. Anwendung finden sollte –, bedarf vielmehr einer differenzierteren Betrachtung anhand der Art der gespeicherten Daten. Insofern ist noch einmal darauf hinzuweisen, dass die Anwendbarkeit des BDSG nur dann gegeben ist, wenn personenbeziehbare Daten verarbeitet werden.

1. Speicherung personenbezogener Daten auf dem Tag

Werden personenbezogene Angaben unmittelbar auf den Tags gespeichert, ist die jeweilige RFID-Applikation daher stets datenschutzrechtlich relevant und fällt eindeutig in den Anwendungsbereich des BDSG. Zu dieser Kategorie zählen gegenwärtig z. B. Ausweis- und Signaturkarten oder personalisierte Veranstaltungstickets.

Die Datenerhebung, -verarbeitung und -nutzung muss in diesen Fällen vollumfänglich den o. g. Vorgaben des BDSG und ggf. einschlägiger bereichsspezifischer Vorschriften genügen.

Werden aktive Tags verwendet, auf denen eigenständige Datenverarbeitungsprozesse stattfinden, sind zudem die besonderen Informationspflichten des § 6c BDSG für mobile personenbezogene Speicher- und Verarbeitungsmedien zu beachten.

2. Speicherung neutraler Daten auf dem Tag

Weniger eindeutig ist die Rechtslage, wenn der Tag neutrale Daten wie eine Kennziffer oder einen Code enthält. In diese Kategorie fallen z. B. RFID-Systeme in den Bereichen Prozesskontrolle, Produktkennzeichnung, Logistik- und Lagermanagement, Zugangskontrolle, Diebstahls- und Fälschungsschutz sowie Tierkennzeichnung. Die Speicherdaten haben in diesen Fällen zwar selbst keinen direkten Personenbezug, dieser kann jedoch gegebenenfalls durch eine Verknüpfung mit personenbezogenen Daten hergestellt werden.

2.1 Unternehmensinterner Bereich

Bei RFID-Anwendungen im rein unternehmensinternen Bereich, d. h. in Fertigung, Logistik oder Lagermanagement, ist eine solche Verknüpfung regelmäßig nicht zu erwarten. Die gespeicherten Daten werden vielmehr dauerhaft nicht personenbezogen bleiben, so dass die Regelungen des BDSG nicht anwendbar sind. Ein besonderer Schutz ist in diesen Fällen aber auch nicht erforderlich, da mangels Personenbeziehbarkeit der verarbeiteten Daten keine Gefahr für das informationelle Selbstbestimmungsrecht Einzelner besteht.

2.2 Verbrauchersphäre

Sobald ein getagtes Objekt in die Sphäre der Verbraucher gelangt, stellt sich die Situation dagegen differenzierter dar.

Zwar muss auch in diesem Fall nicht zwingend eine Verknüpfung zwischen den gespeicherten Daten und einer konkreten Person entstehen. Aufgrund der bereits beschriebenen Besonderheiten von RFID-Systemen ist es jedoch nicht auszuschließen, dass die neutralen Produktcodes zu irgendeinem Zeitpunkt gezielt oder zufällig mit den persönlichen Angaben von Verbrauchern kombiniert und dadurch personenbeziehbar werden. Bei RFID-gestützter Verarbeitung im Verbraucherbereich sind daher auch an sich nicht personenbezogene Daten zumindest „potentiell personenbeziehbar“.

Eine gezielte Verknüpfung geschieht beispielsweise, wenn Verbraucher ein getagtes Produkt mit Kunden- oder Kreditkarte bezahlen und der Produktcode im Back-end-System des Einzelhändlers mit den Kartendaten der Kunden zusammengeführt wird.

Eine zufällige Verknüpfung kann vor allem dadurch entstehen, dass Lesegeräte nicht nur die Tags des aktuellen Einkaufs, sondern auch ältere oder fremde Chips erfassen, die Konsumenten – möglicherweise unbewusst – bei sich tragen.

So ist es beispielsweise denkbar, dass Kunden in der Kleidung Tags aus früheren Einkäufen mit sich führen, für die im Back-end-System des Einzelhändlers bereits eine Verknüpfung existiert. Selbst wenn Kunden bei späteren Einkäufen bar bezahlen, könnten sie über die alten Tags identifiziert werden. Eine persönliche Zuordnung der bar bezahlten Waren wäre dann ebenfalls möglich. Zudem ist nicht ausgeschlossen, dass die Produktcodes fremder Waren ebenfalls ausgelesen und mit vorhandenen personenbezogenen Angaben verknüpft werden. Auf diese Weise wäre es möglich, heimliche Konsum- und Bewegungsprofile zu erstellen, denn insbesondere genormte Kennziffern wie der European Product Code (EPC) lassen anhand ihrer Zeichenfolge – zumindest für andere Lizenznehmer – ohne größeren Aufwand einen Rückschluss auf die Art der getagten Ware zu.

Denkbar ist zudem die Variante, dass der Personenbezug über zufällig ausgelesene Tags mit personenbezogenen Speicherdaten (z. B. Ausweis- oder Signaturkarten) zustande kommt. Allerdings setzen die Verwender solcher Systeme in aller Regel hinreichende Verschlüsselungstechniken ein, um ein Auslesen durch Dritte zu verhindern.

Bei gezielter Verknüpfung wird der Umgang mit den ursprünglich neutralen Daten ab Eintritt der Personenbeziehbarkeit vom BDSG erfasst. Die Erhebung, Verarbeitung und Nutzung der entsprechenden Daten ist dann nur noch unter Beachtung der gesetzlichen Vorgaben zulässig.

Bei zufälliger Verknüpfung ist dagegen zu differenzieren. Das bloße zufällige Auslesen fremder Tags stellt mangels Zielgerichtetheit noch keine Datenerhebung nach dem

BDSG dar. Werden die ausgelesenen Daten jedoch weiterverarbeitet, z. B. automatisiert gespeichert, finden die datenschutzrechtlichen Bestimmungen ab diesem Zeitpunkt Anwendung. Da die Betroffenen bei zufälliger Datenerhebung regelmäßig nicht eingewilligt haben, bedeutet dies, dass die Daten sofort zu löschen sind, § 20 Abs. 2 Nr. 1, § 35 Abs. 2 Satz 2 Nr. 1 BDSG.

Rein rechtlich betrachtet sind die datenschutzrechtlichen Verpflichtungen, denen die Verwender von RFID-Systemen unterliegen, damit eindeutig festgelegt. Eine Personalisierung gespeicherter Daten darf nur dann erfolgen, wenn ein gesetzlicher Erlaubnistatbestand eingreift oder die Betroffenen zuvor eingewilligt haben. Heimliche Profilbildung muss unterbleiben. Zufällig erhobene personenbeziehbare Daten sind zu löschen. Die verantwortliche Stelle muss ihren Aufklärungs- und Informationspflichten genügen und den Betroffenen die Möglichkeit geben, die über sie gespeicherten Daten einzusehen und ggf. löschen oder berichtigen zu lassen. Die hierzu erforderlichen technischen Einrichtungen lassen sich in der Regel ohne weiteres in die jeweiligen RFID-Systeme integrieren, bedeuten für die verantwortlichen Stellen jedoch einen nach den Umständen ggf. nicht unbeträchtlichen finanziellen Aufwand.

Faktisch wird der datenschutzkonforme Einsatz von RFID jedoch dadurch erschwert, dass die Beteiligten – bei zufälligem Auslesen – oftmals nicht rechtzeitig erkennen und kontrollieren können, ob, wann, wo und in welchem Umfang neutrale Daten personenbeziehbar werden und mithin die Einhaltung der gesetzlichen Bestimmungen erforderlich wäre.

Erschwerend kommt hinzu, dass potentielle Personenbeziehbarkeit nicht ausreicht, um das BDSG zur Anwendung zu bringen. Dadurch bewegen sich die Beteiligten gewissermaßen in einer Grauzone. Verwender, die mit RFID gekennzeichnete Produkte in Umlauf bringen, verarbeiten lediglich potentiell personenbeziehbare Produktcodes und unterliegen damit (noch) keinen datenschutzrechtlichen Verpflichtungen. Der Betreiber des Systems, das diese Daten später mit den persönlichen Daten von Verbrauchern verknüpft, hat die Schutzvorschriften des BDSG zwar einzuhalten, kann dies aber faktisch nur in den Fällen tun, in denen – wie etwa beim Bezahlvorgang mit Kreditkarte – die Entstehung des Personenbezugs für ihn rechtzeitig erkennbar wird.

C. Lösungsmöglichkeiten

Effektiver Datenschutz sollte daher beim Einsatz von RFID möglichst frühzeitig einsetzen. Erforderlich sind präventive Maßnahmen zum Schutz des informationellen Selbstbestimmungsrechts ab dem Zeitpunkt, in dem ein getagter Gegenstand – und sei dieser auch nur mit einem Produktcode markiert – in die Verbrauchersphäre gelangt.

Diese präventiven Schutzmaßnahmen sollten in jedem Falle folgende Komponenten beinhalten:

Transparenz und Kennzeichnungspflicht

Der Verbraucher muss auf den Einsatz und die Funktionsweise von RFID-Technologie hingewiesen und umfassend über Art und Verwendungszweck der auf den Chips gespeicherten Daten, einschließlich der vorgesehenen Verknüpfung mit anderen, insbesondere personenbezogenen Daten, informiert werden. Dies kann beispielsweise durch Logos auf den getagten Produkten, Hinweistafeln und Leseterminals zum Abrufen der gespeicherten Daten geschehen. Standort und Reichweite von Readern sind ebenfalls deutlich zu kennzeichnen.

Verbindlicher Verzicht auf heimliche Profilbildung

Es ist zu gewährleisten, dass aus potentiell personenbeziehbaren Speicherdaten wie Produktcodes keine allgemeinen Verhaltens-, Nutzungs- und Bewegungsprofile erstellt werden, da die Gefahr besteht, dass diese später ggf. mit einer konkreten Person in Verbindung gebracht werden können. Zudem wird in diesem Zusammenhang häufig auch ein ausdrückliches Verbot der Bildung unmittelbar personenbezogener Profile gefordert. Ein solches Verbot besteht nach gegenwärtiger Rechtslage jedoch bereits, soweit Betroffene der entsprechenden Verwendung ihrer Daten nicht ausdrücklich zugestimmt haben.

Datensicherheit

Die gespeicherten Daten sind durch geeignete Datensicherheitstechniken vor heimlichem oder zufälligem Auslesen durch Dritte sowie vor unbefugter Veränderung zu schützen. Gleiches gilt für das unbefugte Abhören während des Übertragungsvorgangs vom Tag zum Reader. Zudem ist sicherzustellen, dass die Back-end-Systeme den Anforderungen des § 9 BDSG genügen.

Deaktivierungsmöglichkeit

Konsumenten müssen beim Erwerb eines getagten Produkts die Möglichkeit erhalten, den Chip entweder selbst zu entfernen, zu deaktivieren bzw. die darauf befindlichen Daten zu löschen oder sie müssen dies vom Verkäufer verlangen können. Vorzugsweise sollte die Deaktivierung dabei nach dem sog. „Opt-in-Modell“ erfolgen. Bei diesem Modell werden die Chip-Daten beim Bezahlvorgang automatisch gelöscht. Möchte der Verbraucher die Funktion des Chips erhalten, z. B. um später tag-gebundene Serviceleistungen wie Bonuspunkte oder erleichterten Umtausch in Anspruch nehmen zu können, muss er der Deaktivierung ausdrücklich widersprechen.

Die Wirtschaft favorisiert dagegen das sog. „Opt-out-Modell“ (wobei jedoch in den aktuellen Testverkaufsstellen ganz überwiegend Opt-in praktiziert wird). Opt-out bedeutet, dass die Deaktivierung nicht automatisch vorgenommen wird, sondern nur dann, wenn der Kunde dies ausdrücklich wünscht. Bei diesem Modell besteht die Gefahr, dass Verbraucher es aus Zeitnot, mangelndem Problembewusstsein oder schlicht Vergesslichkeit unterlassen, die Deaktivierung zu verlangen oder durchzuführen.

In jedem Falle sollte die verantwortliche Stelle zudem Leseterminals zur Verfügung stellen, über die Verbraucher den Erfolg der Deaktivierung bzw. den Inhalt der Speicherdaten kontrollieren können.

Datensparsamkeit

Die Reichweite von RFID-Systemen ist auf das erforderliche Maß zu beschränken. Insbesondere ist sicherzustellen, dass möglichst keine Chips fremder Verwender erfasst bzw. die erfassten fremden Speicherdaten umgehend gelöscht werden.

Technische Lösungen zur Gewährleistung dieser Schutzmaßnahmen sind auf dem Markt in unterschiedlicher Form erhältlich bzw. lassen sich auf die jeweilige Applikation zuschneiden. Bei einigen Konsumgütern dürfte es sogar bereits genügen, den Chip so anzubringen, dass er sich körperlich entfernen lässt. In anderen Fällen können die Chips z. B. über sog. Kill-Befehle deaktiviert oder durch Blocker-Tags vor unbefugtem Auslesen abgeschirmt werden.

Es sind zudem Chips mit abtrennbarer Antenne auf dem Markt, die nach dem Entfernen des Antennenteils nur noch im absoluten Nahbereich arbeiten. Diese Chips haben den Vorteil, dass sie von dritter Seite nicht mehr ausgelesen werden können, aber Kunden etwaige tag-gebundene Serviceleistungen des Verwenders erhalten bleiben.

Die zufällige Miterfassung fremder Tags lässt sich in vielen Fällen dadurch verhindern, dass die Reichweite von Lesegeräten auf das absolut notwendige Maß beschränkt wird. Dennoch ausgelesene fremde Speicherdaten können über entsprechende Softwarekomponenten erkannt und automatisch gelöscht werden.

Unterschiedliche Verschlüsselungstechniken zur Gewährleistung ausreichender Datensicherheit stehen ebenfalls zur Verfügung.

Allerdings sind die meisten technischen Lösungen derzeit noch vergleichsweise teuer und aufwändig zu installieren. Dieses Problem würde sich jedoch bei entsprechender Nachfrage entschärfen.

IV. Teil 3: Aktuelle Aktivitäten auf nationaler und europäischer Ebene

Der datenschutzrechtliche Rahmen für den Einsatz von RFID-Technologie wird derzeit auf nationaler wie europäischer Ebene diskutiert.

A. Aktivitäten auf nationaler Ebene

1. Wirtschaft

Die deutsche Wirtschaft zeigt im Hinblick auf die genannten datenschutzrechtlichen Risiken deutliches Problembewusstsein. Kaum eine andere Technologie hat bereits so weit im Vorfeld flächendeckender Anwendung ähnlich große Informations- und Diskussionsbereitschaft ausgelöst wie RFID. Zu den diesbezüglichen Aktivitäten der Wirtschaft zählen Verbraucherinformations-Foren ebenso wie die regelmäßige Teilnahme an Arbeitskreisen, Workshops und bilateralen Gesprächen (u. a. auch mit dem Bundesministerium des Innern und dem Bundesministerium für Wirtschaft und Technologie).

Darüber hinaus haben einige Wirtschaftsverbände und wirtschaftsnahe Forschungseinrichtungen Empfehlungen zum Umgang mit der datenschutzrechtlichen Problematik von RFID erarbeitet (darunter die Internationale Handelskammer, die Europäische Experten Gruppe für IT-Sicherheit und das US-amerikanische Zentrum für Demokratie und Technologie). Derzeit wohl am weitgehendsten sind die Richtlinien von EPCglobal. Danach sollen EPC-Lizenznehmer getagte Waren mit einem EPC-Logo versehen, den Konsumenten über die allgemeine Funktionsweise von RFID einschließlich der bestehenden Deaktivierungsmöglichkeiten aufklären, bei der Verarbeitung EPC-spezifischer Daten die geltenden Rechtsvorschriften einhalten und an der Weiterentwicklung verbraucherfreundlicher Anwendungsalternativen mitwirken.

Darüber hinaus ist derzeit eine Selbstverpflichtung des deutschen Handels in Vorbereitung, die ähnliche Vorgaben enthalten soll. Verbraucherschutzverbände und Wirtschaftsvertreter haben sich bislang allerdings weder über effektive Sanktionsmechanismen noch über die Ausgestaltung der Deaktivierungsmöglichkeiten („Opt-in“- oder „Opt-out-Modell“) einigen können. Angeboten wurden von Seiten des Handels bisher ein Beirat als Kontrollinstanz, Rückgriffsmöglichkeiten im Rahmen des EPC-Netzwerks sowie das „Opt-out-Modell“. Die Ablehnung von „Opt-in“ wird insbesondere damit begründet, dass die Ausgestaltung der handelsspezifischen RFID-Anwendungen noch nicht konkret feststehe und man daher mit möglicherweise kostenintensiven Zugeständnissen vorsichtig sein müsse. Es ist jedoch nahe liegend, dass hinter dem Beharren auf „Opt-out“ auch betriebswirtschaftliche Überlegungen vermutet werden müssen. Andererseits ermöglicht die frühzeitige Vereinbarung eines grundsätzlichen „Opt-in“, dass direkt entsprechende flächendeckende Lösungen entwickelt werden können. Dies würde zugunsten der Unternehmen ggf. zu erheblich reduzierten Investitionskosten gegenüber einer späteren oder sektoralen „Opt-in“ Lösung führen.

2. Bundesregierung

Die Bundesregierung beobachtet seit Jahren aufmerksam die datenschutzrelevanten Entwicklungen im Bereich RFID und steht mit den betroffenen Kreisen in Wirtschaft, Daten- und Verbraucherschutz in regelmäßigem Dialog.

Zur Erstellung dieses Berichts hat das Bundesministerium des Innern (BMI) zahlreiche Einzelgespräche mit den führenden Herstellern und Verwendern von RFID sowie mit verschiedenen Verbraucherschutzverbänden geführt. Zudem hat das BMI dem Bundesamt für Sicherheit in der Informationstechnik (BSI) den Auftrag zur Erstellung „Technischer Richtlinien für den sicheren RFID-Einsatz“ erteilt.

Des Weiteren hat das Bundesministerium für Wirtschaft und Technologie (BMWi) anlässlich der deutschen Ratspräsidentschaft im Juni 2007 eine internationale Konferenz zu den technischen und rechtlichen Aspekten von RFID veranstaltet, an der Repräsentanten aus Politik, Wirtschaft, Wissenschaft, Forschung, Daten- und Verbraucherschutz teilgenommen haben. Die Ergebnisse dieser Konferenz sind in einem vom BMWi erstellten Positionspapier (European Policy Outlook RFID) festgehalten, das zur Frage des Daten- und Verbraucherschutzes folgende Empfehlungen enthält:

– verstärkte Information der Bürger,

– Identifizierung eines etwaigen Gesetzgebungsbedarfs, vorzugsweise jedoch Marktregulierung durch Selbstverpflichtungen der Wirtschaft,

– Entwicklung eines rechtlichen Rahmens auf EU-Ebene.

Zudem setzt sich die Bundesregierung auch in den entsprechenden EU-Gremien aktiv für eine datenschutzkonforme Ausgestaltung von RFID ein.

B. Aktivitäten auf europäischer Ebene

Die EU-Kommission hat am 15. März 2007 eine Mitteilung zur Funkfrequenz-kennzeichnung (RFID) in Europa vorgelegt [KOM(2007) 96 endg.]. Zielsetzung ist die Entwicklung eines ordnungspolitischen Rahmens für eine breite Einführung von RFID.

Der Schwerpunkt der genannten Kommissionsmitteilung liegt vorwiegend auf den technischen und wirtschaftlichen Aspekten von RFID. Im Hinblick auf datenschutzrechtliche Belange werden die Mitgliedstaaten zur Ergreifung von Aufklärungs- und Informationskampagnen und zur ständigen Beobachtung, Bewertung, Lenkung und Regulierung der Technologie aufgefordert. Die Frage nach der Notwendigkeit von Leitlinien wird angesprochen, aber im Ergebnis offen gelassen. Bevor weitergehende Regelungen auf europäischer Eben vorgeschlagen werden, soll der Dialog mit relevanten Interessengruppen vertieft werden.

Vor diesem Hintergrund prüft die Kommission derzeit unter Beteiligung der Artikel-29-Datenschutzgruppe, ob und ggf. welche zukünftigen gesetzgeberischen Maßnahmen zur Einhaltung des Datenschutzes im Zusammenhang mit RFID erforderlich sind. Mit Beschluss vom 28. Juni 2007 hat sie zudem eine paritätisch besetzte RFID-Expertengruppe berufen (2007/467/EG). Diese wird 2008 Leitlinien zu Sicherheit und Datenschutz beim Einsatz von RFID veröffentlichen.

Zudem hat im Rahmen der portugiesischen Ratspräsidentschaft am 15./16. November 2007 eine weitere europäische Konferenz zu den aktuellen Entwicklungen im RFID-Bereich stattgefunden, an der seitens der Bundesregierung das BMI teilgenommen hat. In datenschutzrechtlicher Hinsicht waren sich die Teilnehmer weitgehend einig, dass eine starre gesetzliche „One size fits all“-Regelung den stark diversifizierten und teilweise noch in der Testphase befindlichen Anwendungsformen von RFID nicht hinreichend Rechnung tragen könne. Vielmehr müssten applikationsspezifische Lösungen gefunden werden – vorzugsweise durch Selbstverpflichtungen der jeweiligen Interessenträger, Sensibilisierung der Betroffenen und die Entwicklung datenschutzfreundlicher Techniken.

V. Teil 4: Handlungsoptionen des Gesetzgebers

Zur Förderung des datenschutzkonformen Einsatzes von RFID-Technologie bieten sich im Wesentlichen drei Möglichkeiten:

– eine Änderung des BDSG,

– die Schaffung einer bereichsspezifischen Regelung außerhalb des BDSG (RFID-Datenschutzgesetz) oder

– die Selbstregulierung des Marktes auf der Grundlage effektiver Selbstverpflichtungen der Wirtschaft.

Ergänzend kommen Aufklärungs- und Informationskampagnen zur Sensibilisierung der Verbraucher in Betracht. Diese könnten ggf. gemeinsam mit den betroffenen Wirtschafts- und Verbraucherschutzkreisen durchgeführt werden.

A. Änderung des BDSG

1. Möglicher Inhalt

Wie bereits dargestellt gelten die Schutzvorschriften des BDSG ausschließlich für den Umgang mit personenbezogenen Daten und sind daher auf die RFID-typische Verarbeitung von Daten mit lediglich potentiellem Personenbezug nicht anwendbar. Ein denkbarer Lösungsansatz wäre insofern die Einbeziehung potentiell personenbeziehbarer Daten in das Schutzregime des BDSG. Ebenfalls zu diskutieren wäre – wie der Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 14. November 2007 (Bundestagsdrucksache 16/7138) anregt – die Festschreibung von Sanktionen für den Fall, dass datenschutzrelevante Selbstverpflichtungen der Wirtschaft nicht eingehalten werden.

2. Bewertung

Für eine Änderung des BDSG in der einen oder anderen Form spricht, dass sie die derzeit bestehende Grauzone bei der Datenverarbeitung mit RFID-Systemen beseitigen würde. Als gesetzliche Verpflichtung wäre sie zudem verbindlich und über die etablierten Kontroll- und Sanktionsmechanismen des BDSG auch praktisch durchsetzbar.

Dagegen spricht, dass das BDSG als technikneutrales Schutzregime konzipiert ist, und sich in dieser Form bewährt hat. Besonderen Risiken einzelner Technologien sollte vorzugsweise im Rahmen bereichsspezifischer Gesetze begegnet werden. Bereichsspezifische Regelungen lassen individuellere und differenziertere Lösungen zu und bergen – im Gegensatz zu einer Änderung des allgemein anwendbaren BDSG – nicht die Gefahr nachteiliger Folgen für andere datenschutzrelevante Felder.

Insofern ist vorliegend vor allem der Bereich der georeferenzierten Daten problematisch. Eine pauschale Einbeziehung potentiell personenbeziehbarer Daten in das BDSG würde nämlich nicht nur für RFID-Systeme sondern möglicherweise auch für die Georeferenzierung gelten. Die datenschutzrechtliche Behandlung georeferenzierter Daten ist jedoch ebenso komplex wie umstritten und bedürfte in jedem Falle einer differenzierteren Betrachtung.

Wollte man eine RFID-spezifische Regelung in das BDSG aufnehmen, dürfte diese mithin nur klar abgrenzbare Aspekte regeln.

Hinzu kommt, dass RFID im datenschutzrelevanten Bereich bislang keine signifikante Verbreitung gefunden hat. Noch weitgehend offen ist derzeit auch, ob und in welcher konkreten Form sich RFID-Systeme in der Verbrauchersphäre durchsetzen werden. Entsprechend lässt sich derzeit noch nicht absehen, welche gesetzliche Regelung Unternehmen und Verbrauchern auf Dauer am besten gerecht wird. Gleichermaßen offen sind Form, Ziel und Inhalt der mittelfristig umzusetzenden europäischen Maßnahmen. Eine starre gesetzliche Regelung müsste daher möglicherweise in nicht allzu ferner Zukunft wieder revidiert werden. Sie würde wenig zur Rechtssicherheit der Betroffenen beitragen, aber umgekehrt von Wirtschaft und Forschung als negatives politisches Signal verstanden. Mithin wäre eine Änderung des BDSG zum jetzigen Zeitpunkt kaum vorteilhaft für die Verbraucher, aber deutlich nachteilig für die internationale Konkurrenzfähigkeit deutscher Unternehmen.

B. Schaffung einer bereichsspezifischen Regelung außerhalb des BDSG

1. Möglicher Inhalt

In einer bereichsspezifischen Regelung – etwa in Form eines RFID-Datenschutz-gesetzes – könnten die bereits erwähnten präventiven Schutzmaßnahmen (Transparenz, Kennzeichnungspflicht, Verzicht auf heimliche Profilbildung, Datensicherheit, Deaktivierungsmöglichkeiten, Datensparsamkeit) differenziert und normenklar geregelt sowie durch effektive Durchsetzungsmechanismen ergänzt werden. Für den Erlass eines RFID-Gesetzes wäre innerhalb der Bundesregierung das Bundesministerium für Wirtschaft und Technologie federführend zuständig.

2. Bewertung

Mit einer bereichsspezifischen Regelung ließe sich die bestehende Grauzone beseitigen, ohne zugleich die Technikneutralität des BDSG anzutasten.

Allerdings hätte ein bereichsspezifisches RFID-Gesetz zum gegenwärtigen Zeitpunkt zum Teil dieselben Nachteile wie eine Änderung des BDSG. Hinzu kommt, dass differenzierte und zumindest mittelfristig sinnvolle Lösungen schwierig sind, so lange noch keine hinreichend verfestigte Anwendungsstruktur oder zumindest eine hinreichend sichere Zukunftsprognose über die Entwicklung einer Technologie vorliegt. Beides ist im Hinblick auf RFID (noch) nicht gegeben. Daher wäre zum gegenwärtigen Zeitpunkt eine nachhaltige und ausgewogene Regelung der RFID-spezifischen Datenschutzproblematik nur schwer zu realisieren.

C. Selbstverpflichtung der Wirtschaft

Alternativ könnte der Gesetzgeber dem Markt daher – zumindest bis sich die datenschutzrelevanten Anwendungsformen von RFID näher konkretisiert haben – eine Chance zur Selbstregulierung geben. Als Regulierungsinstrumente kämen vor allem Selbstverpflichtungen der betroffenen Wirtschaftskreise in Betracht.

1. Möglicher Inhalt

Inhaltlich wäre insofern zu fordern, dass diese Selbstverpflichtungen zum einen den oben unter Ziff. III C genannten Kriterien entsprechen und zum anderen wirksame Sanktionsmechanismen beinhalten. Zudem müsste – insbesondere in sensiblen Bereichen – eine Deaktivierung nach dem Opt-in-Modell gewährleistet sein. Sensibel erscheinen vor allem Anwendungen auf Trägerobjekten, die im Falle der Verknüpfung mit einer Person mittelbar oder unmittelbar Rückschlüsse auf besondere Arten personenbezogener Daten i. S. d. § 3 Abs. 9 BDSG zulassen (rassische und ethnische Herkunft, politische, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben). Als sensibel wären zudem solche Trägerobjekte einzustufen, die der Betroffene typischerweise über längere Zeit bei sich führt. Bei letzteren besteht nämlich – anders als etwa bei Produkten, die zügig verbraucht oder überwiegend im häuslichen Bereich aufbewahrt werden – eine erhöhte Gefahr, dass der Betroffene mit ihnen erneut in den Lesegerät eines RFID-Systems gelangt, das geeignet ist, die gespeicherten Daten unbemerkt auszulesen und mit seiner Person zu verknüpfen. In zeitlicher Hinsicht sollten Selbstverpflichtungen noch in der Testphase der jeweiligen Anwendung abgeschlossen werden, d. h. bevor der Einsatz von RFID auf dem betreffenden Gebiet in regelmäßige Anwendungsstrukturen übergeht, bzw. kritische Verbreitung findet.

2. Bewertung

Für eine solche Vorgehensweise spricht vor allem die Flexibilität von Selbstverpflichtungen. Im Gegensatz zu starren gesetzlichen Regelungen erlauben sie differenziertere bereichsspezifische Lösungen, sind offener für neue datenschutzrelevante Entwicklungen und schränken dadurch die Wettbewerbsfähigkeit und das Innovationspotential der betroffenen Unternehmen weniger ein.

Die betroffenen Wirtschaftskreise zeigen sich in Bezug auf die datenschutzrechtlichen Risiken von RFID auch durchaus problembewusst. Keine andere Technologie hat bereits so weit im Vorfeld flächendeckender praktischer Anwendbarkeit eine vergleichbare Informations- und Diskussionsbereitschaft ausgelöst.

Auf der anderen Seite ist jedoch darauf hinzuweisen, dass die bisherigen Selbstverpflichtungsansätze noch in einigen Punkten hinter den eingangs genannten Mindeststan-

dards zurückbleiben. Weder die Richtlinien von EPCglobal noch die aktuell diskutierte Selbstverpflichtung des Handels sehen effektive Sanktionsmechanismen vor. Zur Kernfrage des Opt-in/Opt-out haben Wirtschaft und Verbraucherschutzverbände sich bislang ebenfalls noch nicht auf eine Lösung einigen können. Ob eine zeitnahe Selbstregulierung des Marktes gelingt, ist daher gegenwärtig völlig offen.

VI. Teil 5: Empfehlung zur weiteren Vorgehensweise

A. Auf nationaler Ebene

Es erscheint vorzugswürdig, zumindest zum gegenwärtigen Zeitpunkt auf eine gesetzliche Regelung zu verzichten und dem Markt zunächst die Chance zur Selbstregulierung zu lassen.

Der damit verbundene geringere Grad an Rechtssicherheit ist insofern hinnehmbar, als RFID-Systeme im datenschutzrelevanten Bereich noch keine kritische Verbreitung gefunden haben und bisher auch noch keine Missbrauchsfälle bekannt geworden sind. Die RFID-gestützte Verarbeitung personenbezogener Daten wird auch mittelfristig kaum über das hinausgehen, was bereits heute über Videoüberwachung und die Verknüpfung von Barcodes und Kreditkartendaten üblich ist. Entsprechend sieht auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) gesetzgeberischen Handlungsbedarf aktuell nur für den Fall, dass die Marktregulierung über effektive Selbstverpflichtungen scheitern sollte (21. Tätigkeitsbericht des BfDI, S. 41 f.). Hinzu kommt, dass zurzeit der zukünftige europäische Rechtsrahmen und die damit verbundenen nationalen Umsetzungserfordernisse noch offen sind.

Eine – zumindest kurz- bis mittelfristige – Zurückhaltung des Gesetzgebers ließe der deutschen Wirtschaft dagegen die Chance, das Innovations- und Gewinnpotential von RFID auch in der nächsten Zeit voll zu nutzen und dadurch ihre internationale Vorreiterstellung zu festigen.

Gleichwohl sollten Bundesregierung und Gesetzgeber die Marktentwicklung und insbesondere das Bemühen der betroffenen Wirtschaftskreise um eine effektive Selbstverpflichtung weiterhin aufmerksam beobachten. Sollte hier in absehbarer Zeit keine Einigung zustande kommen, wäre zu prüfen, ob nicht – zumindest für die o. g. sensiblen Bereiche – die Deaktivierung nach dem opt-in-Modell – etwa durch eine Änderung des BDSG – gesetzlich geregelt werden müsste.

Im Übrigen ist der gesetzgeberische Handlungsbedarf spätestens dann erneut zu prüfen, wenn sich die Anwendungsstrukturen im Endkundenbereich konkretisieren, bzw. RFID in der Verbrauchersphäre einen größeren Verbreitungsgrad erreicht, oder wenn der zukünftige europäische Rechtsrahmen absehbar wird. Des weiteren wird darauf zu achten sein, ob bei der technischen Weiterentwicklung von RFID die oben genannten präventiven Schutzmaßnahmen beachtet werden. Darüber hinaus könnte es sich empfehlen, den Verbraucher – etwa durch Sensibilisierungskampagnen – vermehrt auf die datenschutzrechtlichen Implikationen von RFID aufmerksam zu machen. Anzudenken wären des Weiteren Fördermaßnahmen zur Entwicklung datenschutzfreundlicher Technologien.

B. In Bezug auf die europäische Ebene

Im Zusammenhang mit der von der Europäischen Kommission in ihrer auf S. 26 zusammengefassten Mitteilung angeregten und eingeleiteten Diskussion zu RFID müssen deutsche Interessen insbesondere hinsichtlich der Ausgestaltung eines europäischen Rechtsrahmens definiert und kommuniziert werden. Dabei sollte das deutsche Interesse insbesondere auch darin bestehen, dass die Verwaltung, Lenkung, Kontrolle und Normung der im Aufbau befindlichen RFID-Infrastruktur in Europa gehalten werden, um so – nicht zuletzt unter datenschutzrechtlichen Gesichtspunkten – bestimmenden Einfluss auf deren Ausgestaltung nehmen zu können.

VII. Zusammenfassung

RFID ist ein Verfahren zur kontaktlosen Identifizierung von Objekten per Funk, bestehend aus zwei Komponenten: einem elektronischen Mikrochip mit Antenne und einem Lesegerät, das die auf dem Chip gespeicherten Daten erfasst und in eine Datenbank überträgt.

RIFD-Technologie bietet großes Potential für Wirtschaft und Verbraucher. Auf Seiten der Unternehmen verspricht sie vor allem Effizienzsteigerungen im Bereich logistischer Prozesse. Die Verbraucher profitieren durch vereinfachte Zahlungsvorgänge und höhere Produktsicherheit. Deutsche Unternehmen sind derzeit als Hersteller und Verwender von RFID-Technologie führend in Europa.

In Logistik und Prozesskontrolle hat RFID bereits signifikante Verbreitung gefunden. Im Endkundenbereich beschränkt sich die Anwendung von RFID-Systemen dagegen noch weitestgehend auf Pilotprojekte. Ein flächendeckender Einsatz ist hier aufgrund der hohen Investitionskosten auch mittelfristig nicht zu erwarten.

Datenschutzrechtliche Risiken entstehen, wenn RFID zur Erhebung, Verarbeitung oder Nutzung personenbeziehbarer Daten eingesetzt wird. Dies ist der Fall, wenn die Chipdaten entweder selbst persönlicher Natur sind oder in der Hintergrunddatenbank des Systems mit personenbezogenen Angaben von Verbrauchern verknüpft werden.

Werden personenbezogene Daten verarbeitet, gelten grundsätzlich die umfassenden Datenschutzrechte des Betroffenen nach dem BDSG. Die praktische Gewährleistung dieser datenschutzrechtlichen Vorgaben wird jedoch durch die besondere Funktionsweise von RFID erschwert. Denn aufgrund der automatischen und sichtkontaktlosen Art der Datenübertragung vom Chip zum Lesegerät ist oftmals nicht ohne weiteres erkennbar, wann, wo und in welchem Umfang ein Personenbezug entsteht.

Daher müsste das informationelle Selbstbestimmungsrecht bei RFID-gestützter Datenverarbeitung durch präventive Schutzmaßnahmen abgesichert werden. Diese

Schutzmaßnahmen sollten Transparenz, Datensicherheit, den Verzicht auf heimliche Profilbildung, Datensparsamkeit sowie – insbesondere für sensible Bereiche – eine Deaktivierung nach dem opt-in-Modell gewährleisten und unabhängig von einer Personenbeziehbarkeit der gespeicherten Daten bereits dann eingreifen, wenn ein getagter Gegenstand in die Verbrauchersphäre gelangt.

Vor einem möglichen gesetzgeberischen Tätigwerden ist aus der Sicht der Bundesregierung jedoch zunächst abzuwarten, ob die genannten Anforderungen des Datenschutzes – insbesondere die Frage des opt-in – auch durch eine zeitnah abzuschließende Selbstverpflichtung der Wirtschaft gewahrt werden und welche Anwendungen sich im Endkundenbereich konkretisieren.

Allerdings ist eine RFID-spezifische Änderung des BDSG schon deshalb nicht empfehlenswert, weil sich die technikneutrale Konzeption dieses Gesetzes stets bewährt hat und daher nicht angetastet werden sollte. Wollte man dennoch eine solche Änderung in das BDSG aufnehmen, wäre daher in jedem Falle zu gewährleisten, dass diese technikneutrale Ausgestaltung nicht grundlegend in Frage gestellt wird.

Eine bereichsspezifische Regelung in Form eines eigenständigen RFID-Gesetzes wäre derzeit ebenfalls nur schwer möglich, da die Anwendungsstrukturen von RFID-Systemen im Verbraucherbereich noch nicht hinreichend absehbar sind. Ebenso offen sind der zukünftige europäische Rechtsrahmen und die damit verbundenen nationalen Umsetzungserfordernisse. Allerdings werden gerade bei der Entwicklung einer Technologie wichtige Weichen gestellt. Daher wären gesetzliche Schritte näher zu prüfen, wenn die genannten präventiven Schutzmaßnahmen bei der technologischen Weiterentwicklung von RFID nicht ausreichend Berücksichtigung finden sollten.

Eine nachhaltige und ausgewogene Regelung erscheint vor diesem Hintergrund momentan nur schwer zu realisieren. Zudem ist zu berücksichtigen, dass RFID derzeit auf Endkundenebene noch keine signifikante Verbreitung gefunden hat.

Eine starre, rein nationale gesetzliche Regelung würde zudem das Innovationspotential und die internationale Wettbewerbsfähigkeit deutscher Unternehmen deutlich einschränken.

Gegenwärtig empfiehlt es sich daher, zunächst auf eine Selbstregulierung des Marktes in Form effektiver Selbstverpflichtungen der betroffenen Wirtschaftskreise zu setzen und diese gegebenenfalls durch Sensibilisierungskampagnen und die Förderung datenschutzfreundlicher Technologien zu unterstützen.

Darüber hinaus sollten Bundesregierung und Gesetzgeber die Marktentwicklung auch weiterhin aufmerksam beobachten, mit den betroffenen Kreisen im Dialog bleiben und den gesetzgeberischen Handlungsbedarf erneut prüfen, wenn sich die datenschutzrelevanten Anwendungen von RFID konkretisiert haben.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333